AENSI Journals

Australian Journal of Basic and Applied Sciences

ISSN:1991-8178

Journal home page: www.ajbasweb.com

Design of a Network Security Tool Using Open-Source Applications

N. Akhyari and S. Fahmy

Faculty of Computer, Media and Technology Management, TATI University College, Teluk Kalong, 24000 Kemaman, Terengganu, MALAYSIA

ARTICLE INFO

Article history:
Received 20 November 2013
Received in revised form 24 January 2014
Accepted 29 January 2014
Available online 5 April 2014

Keywords:
Network Security Tool; Network Defender; Open-Source Application; Firewall, Network Intrusion Detection; Vulnerability Scanner; Exploit Tool

ABSTRACT

Network Security is a crucial aspect in network management with many organizations around the world spend millions each year to safeguard valuable corporate data and information. Many companies use firewalls and encryption mechanisms as security measure. Although there are many types of firewalls and encryption mechanisms in the market, not all are suitable for *Small and Medium Enterprises* (SMEs). For SMEs, these applications might be an overkill, both financially and functionally. This paper proposes the design of *Network Defender*, a network security tool, based on open-source applications. Network Defender is composed of four components namely *Firewall*, *Network Intrusion Detection*, *Vulnerability Scanner*and *Exploit Tool*. The feasibility of this design was demonstrated by the implementation of Network Defender using *PfSense*, *Snort,Nmap*and *Metasploit*. Test results show that all four components work well together in detecting and disabling network attacks. The use of Metasploit also enable reverse attacks to be carried out.

To Cite This Article: N. Akhyari and S. Fahmy., Design of a Network Security Tool Using Open-Source Applications. ***Aust. J. Basic & Appl. Sci.,*** *8(4): 40-46, 2014*

INTRODUCTION

Network Security is a crucial aspect in network management with many organizations around the world spend millions each year to safeguard valuable corporate data and information. Academic and commercial research efforts in this field are heading towards the development of a better security technology. The structure of the Internet itself, is not without fault, presenting security threats not only from outside, but also from within the network. Typical network attacks include *eavesdropping, Denial-of-Service, buffer overflow* and *Structured Query Language Injection*. These attacks might result in a simple identity theft to loss of lives.

Many companies use firewalls and encryption mechanisms as a security measure (BhavyaDaya, 2013). Although there are many types of firewalls and encryption mechanisms in the market, not all are suitable for small companies such as the *Small and Medium Enterprises* (SMEs). For SMEs, these applications might be an overkill, both financially and functionally.As such, this study aims to propose the design of a network security tool based on open-source applications for SMEs.

2. Similar Products:

This section presents review of similar network security product found in the market. The aim of this review is to identify crucial components in a security application, thus, serving as a basis for the design of a network security tool for SMEs. Among the products include *SecureHost, RealSecure Server Sensor, Radware's Attack Mitigation System (AMS), Sourcefire Next-Generation IPS* and *StillSecure Border Guard.*

SecureHost:

SecureHost uses SSH connection and is capable of detecting an attack and provide appropriate reaction ("SecureHost," 2013). Its *Intrusion SecureHost Agent* studies the server's specific applications' behaviour, and automatically detect, prevent and notify the *SecureHost Console* of possible attacks. The *SecureHost Console* deploys *SecureHost Agents* to host systems, collects attack and system alerts and notifies system administrators via a variety of alert channels. *SecureHost Console* communicates with *SecureHost Agents* via authenticated encrypted connections enabling easy remote management and deployment across routers, firewalls and distributed networks. *SecureHost Console* reports alerts in real time and historically, and segments alerts across protected machines and applications. Each alert can be individually examined and correlated to contemporary system and application log data, network connections and file access history facilitating alert forensics.This

Corresponding Author: N. Akhyari, Faculty of Computer, Media and Technology Management, TATI University College, Teluk Kalong, 24000 Kemaman, Terengganu, MALAYSIA.
E-mail: akhyari@tatiuc.edu.my

system has two main components: *Intrusion SecureHost Agent* and *SecureHost Console*, both are classified as a *Network Intrusion Detection*.

RealSecure Server Sensor:

RealSecure uses SSH connection and inspects incoming network traffic. It has a powerful log monitoring capability where it scans the log files and search for known text patterns or rules ("IBM Internet Security Systems," 2013). Once a possible attack is detected, it sends out an alert message either to an individual or another system. *RealSecure Server Sensor* pre-emptively combats threats and addresses vulnerabilities at the network level while performing security compliance auditing. *RealSecure Server Sensor* protects against network vector attacks including worms, bot worms, trojans and Denial-of-Service attacks through a local firewall and inline vulnerability-centric intrusion prevention. This system has two main components: N*etwork Intrusion Detection and Firewall.*

Radware's Attack Mitigation System (AMS):

Radware's (AMS) is a real-time network and application attack mitigation that protects the application infrastructure against network and application downtime, application vulnerability exploitation, malware spread, information theft, web service attacks and web defacement ("Radware," 2013). This system contains four key components: *Network Behavioral Analysis*, *Intrusion Prevention System*, *Reputation Engine* and *Web Application Firewall*, which can be classified as *Firewall* and *Netwok Intrusion Detection*.

Sourcefire Next-Generation IPS:

Sourcefire Next-Generation IPS is a system that provide advanced threat protection, integrating real-time contextual awareness, intelligent security automation, and unprecedented performance with network intrusion prevention ("Sourcefire NGIPS/NGFW," 2013). Its passive intrusion detection mode notifies of suspicious network traffic and behavior while inline IPS mode blocks threats. This system can be further expanded with optional subscription licenses to add *Application Control/URL Filtering* and *Advanced Malware Protection*. The components in this system can be classified as *Firewall* and *Netwok Intrusion Detection*.

StillSecure Border Guard:

This system identifies, profiles and displays attacks on networks by using its Web-based interface. Through Latis' *Dynamic Attack Suppression* technology, *Border Guard* automatically takes action against attacks by ordering the firewall to block malicious traffic that would otherwise be allowed through ("StillSecure," 2013). It can also notify via email or pager, send an SNMP trap or execute a custom script. *StillSecure Border Guard* responds to intrusions that match its continuously updated directory of rules as well as anomalous traffic patterns. It features comprehensive research and advice to help determine how to respond to specific attacks. A robust database is included to ensure the logging of all network activity, and *Border Guard's* built-in reporting engine offers a wide range of customizable, actionable reports. *Border Guard* is managed by the *StillSecure Console* and features multi-user management of all instances of the product throughout the network.The components in this system can be classified as *Firewall* and *Netwok Intrusion Detection*.

Discussions in this section has revealed that the two most important component in a network security application are *Firewall* and *Network Intrusion Detection*. However, the authors argue that in order to cope with escalating network attacks, two other components should be included namely *Vulnerability Scanner* and *Exploit Tool*.

3. Design of Network Security Tool:

This section presents a design for *Network Defender*, a network security tool. Network Defender is composed of four components namely *Firewall*, *Network Intrusion Detection*, *Vulnerability Scanner* and *Exploit Tool*. *Firewall* is a software or hardware-based network security system that controls incoming and outgoing traffic by analyzing data packets. Firewall determines which traffic should be allowed to pass or rejected, based on a set of rules ("Firewall," 2013). It also establishes a barrier between a trusted and secure, internal network and other networks. *Network Intrusion Detection System* (NIDS) is a system that attempts to discover unauthorized access to a computer network by analyzing traffic for signs of malicious activity ("Network Intrusion Detection System," 2013). *Vulnerability Scanner* is a computer program designed to assess computers, systems, networks or applications for weaknesses. There are many types of scanners found in literature, based on focus and particular targets. While the functionality varies between different types of scanners, they share a common, core purpose of enumerating vulnerabilities in one or more targets. *Exploit Tool* is used for developing and executing exploit code against a remote target.

4. Implementation:

This section presents the configuration and integration of open-source applications in the development of *Network Defender*, a network security tool. *Network Defender* comprises of four distinct, yet related, applications: *Firewall*, *Vulnerability Scanner*, *NIPS* and *Exploit Tool*.

After considering many open-source firewalls, *PfSense* is chosen for the firewall component. PfSense is a open source firewall/router distribution based on FreeBSD. PfSense can be deployed as a *Perimeter Firewall*, *router*, *DHCP server*, *DNS server*, and as a VPN endpoint (“PfSense,” 2013). PfSense acts a router, providing IP addresses to other server.

Snort is used as NIDS in Network Defender. Snort is an open-source Network Intrusion Prevention System and Network Intrusion Detection System, capable of performing packet logging and real-time traffic analysis on networks (“SNORT,” 2013). It can carry out protocol analysis; content searching/ matching; and is commonly used to actively block or passively detect a variety of attacks and probes, such as buffer overflows and web application attacks.

The *Vulnerability Scanner* is made up by *Nmap*. Nmap is a security scanner written by Gordon Lyon used to discover hosts and services on a network, creating a map of the network. Nmap uses IP packets to determine available hosts on the network; services offerred by the hosts; operating systems used; type of packet filters/ firewalls used, and others. In Network Defender, Nmap is used to analyze the characteristics of an attacking IP address including operating system information and ports used.

Finally, the *Exploit Tool* component is based on *Metasploit*. Metasploit is an open-source computer security project which provides information on security vulnerabilities. It also supports penetration testing and IDS signature development. Its most well-known sub-project is the *Metasploit Framework*, a tool for developing and executing exploit code against a remote target machine. Metasploit is used to execute exploit codes to disable an attack.

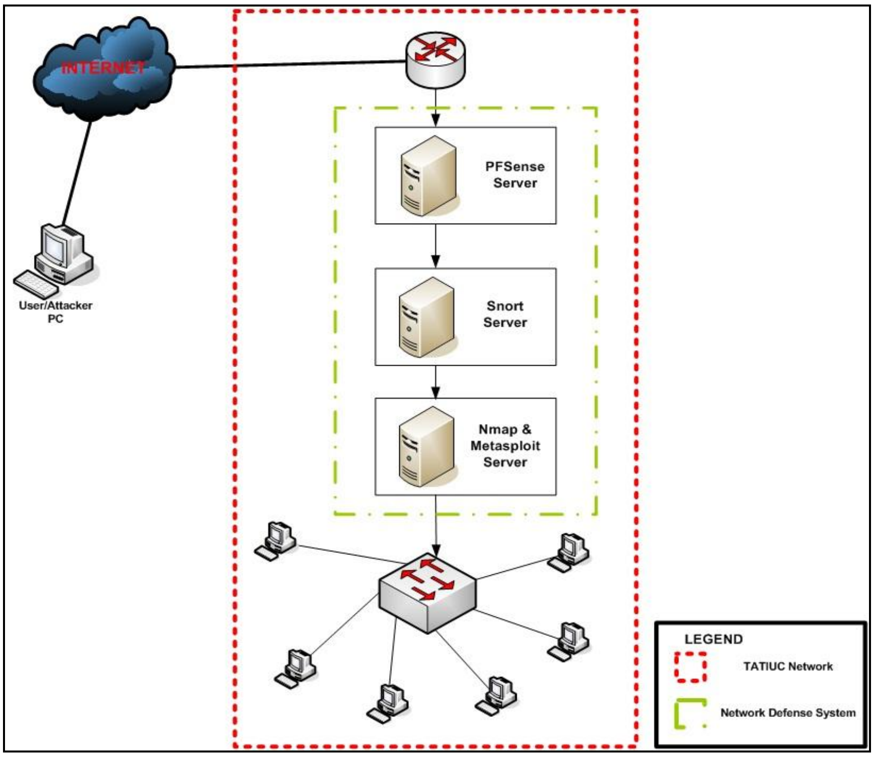


Fig. 1: Logical Layout of Network Defender.

The logical design of Network Defender on the Ubuntu Linux platform is illustrated in Fig. 1. The layered approach supports two major processes. The first process is data transmission from one layer to another. PfSense (firewall), filters all incoming and outgoing packets then pass it to Snort, followed by Nmap, and finally Metasploit. The second process is disabling attacks. Network Defender uses the information from Nmap and attempts to disable attacks using Metasploit.These processes are illustrated in Fig. 2.

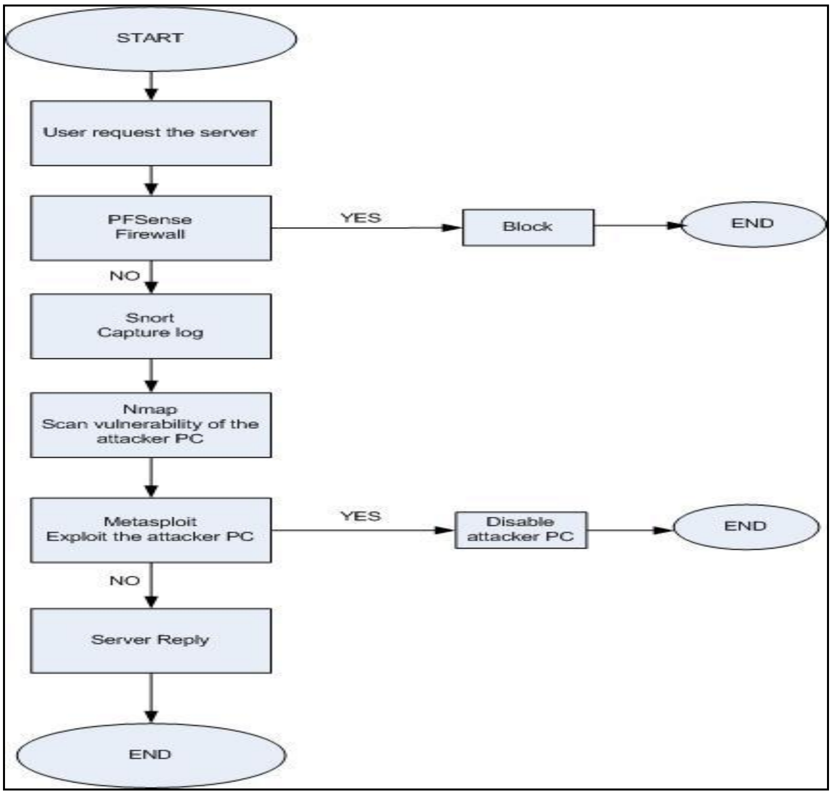
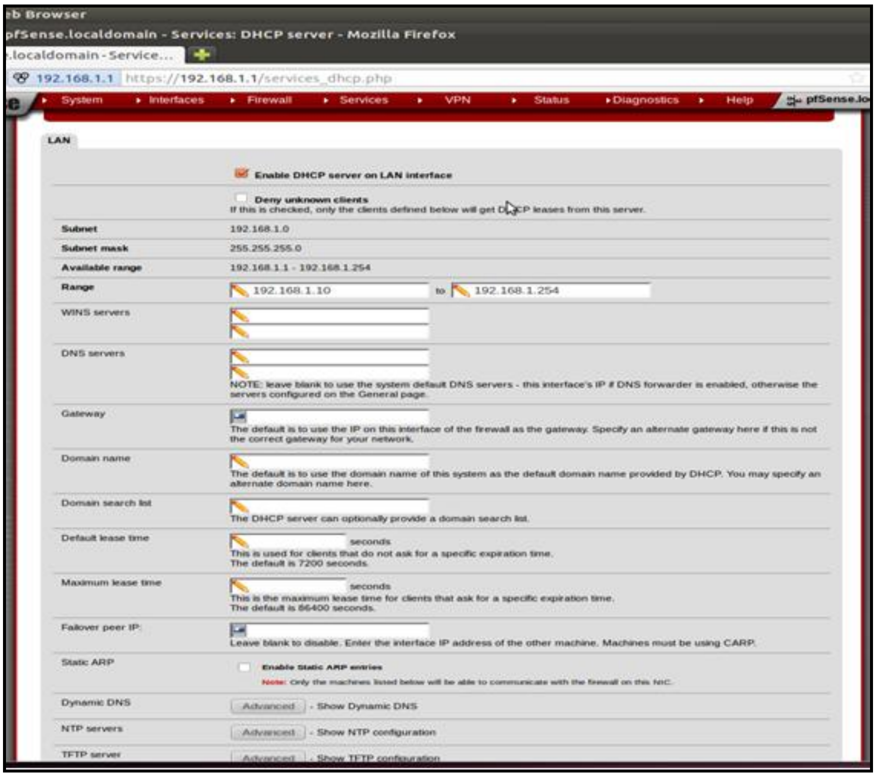


Fig. 2: Process Flow in Network Defender.

Testing:

This section presents the procedures carried out to Network Defender to test its functionality and feasibility as a network security tool.



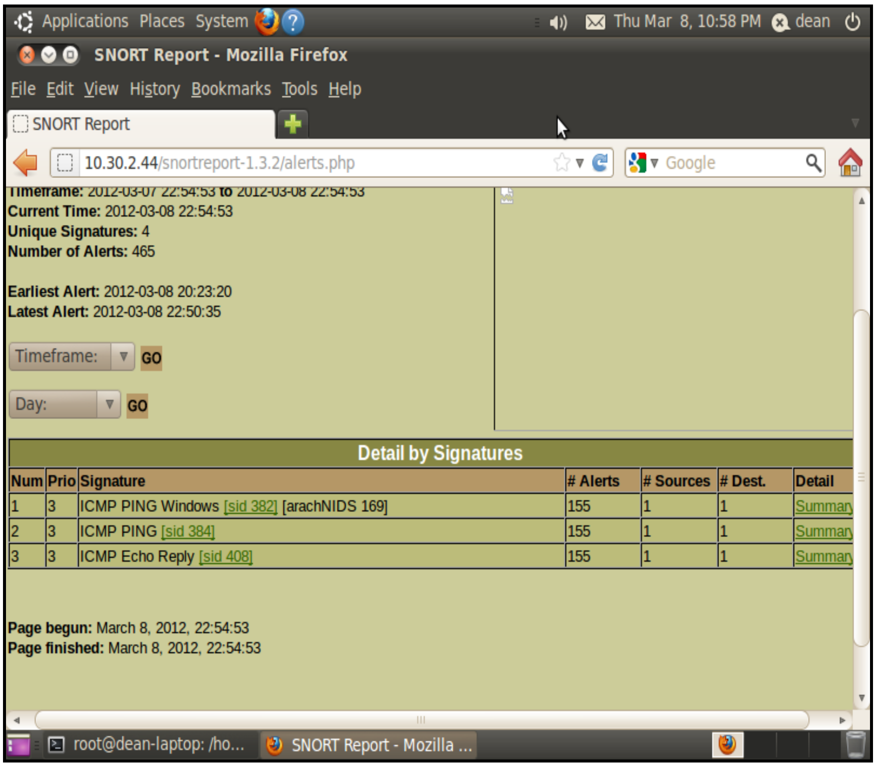
https://192.168.1.1/services_dhcp.php

LAN

	☑ **Enable DHCP server on LAN interface**
	□ **Deny unknown clients** If this is checked, only the clients defined below will get DHCP leases from this server.
Subnet	192.168.1.0
Subnet mask	255.255.255.0
Available range	192.168.1.1 - 192.168.1.254
Range	192.168.1.10 to 192.168.1.254
WINS servers	
DNS servers	NOTE: leave blank to use the system default DNS servers - this interface's IP if DNS forwarder is enabled, otherwise the servers configured on the General page.
Gateway	The default is to use the IP on this interface of the firewall as the gateway. Specify an alternate gateway here if this is not the correct gateway for your network.
Domain name	The default is to use the domain name of this system as the default domain name provided by DHCP. You may specify an alternate domain name here.
Domain search list	The DHCP server can optionally provide a domain search list.
Default lease time	seconds This is used for clients that do not ask for a specific expiration time. The default is 7200 seconds.
Maximum lease time	seconds This is the maximum lease time for clients that ask for a specific expiration time. The default is 86400 seconds.
Failover peer IP:	Leave blank to disable. Enter the interface IP address of the other machine. Machines must be using CARP.
Static ARP	□ **Enable Static ARP entries** **Note:** Only the machines listed below will be able to communicate with the firewall on this NIC.
Dynamic DNS	Advanced - Show Dynamic DNS
NTP servers	Advanced - Show NTP configuration
TFTP server	Advanced - Show TFTP configuration

Fig. 3: PfSense Configuration.

The test on PfSense reveals that it is capable for assigning IP address using DHCP and capable of translating external IP address using NAT (Fig. 3).


Applications Places System
Thu Mar 8, 10:58 PM dean
SNORT Report - Mozilla Firefox
File Edit View History Bookmarks Tools Help
SNORT Report
10.30.2.44/snortreport-1.3.2/alerts.php
Google
Timeframe: ▾ GO
Day: ▾ GO
root@dean-laptop: /ho...
SNORT Report - Mozilla ...

Timeframe: 2012-03-07 22:54:53 **to** 2012-03-08 22:54:53
Current Time: 2012-03-08 22:54:53
Unique Signatures: 4
Number of Alerts: 465

Earliest Alert: 2012-03-08 20:23:20
Latest Alert: 2012-03-08 22:50:35

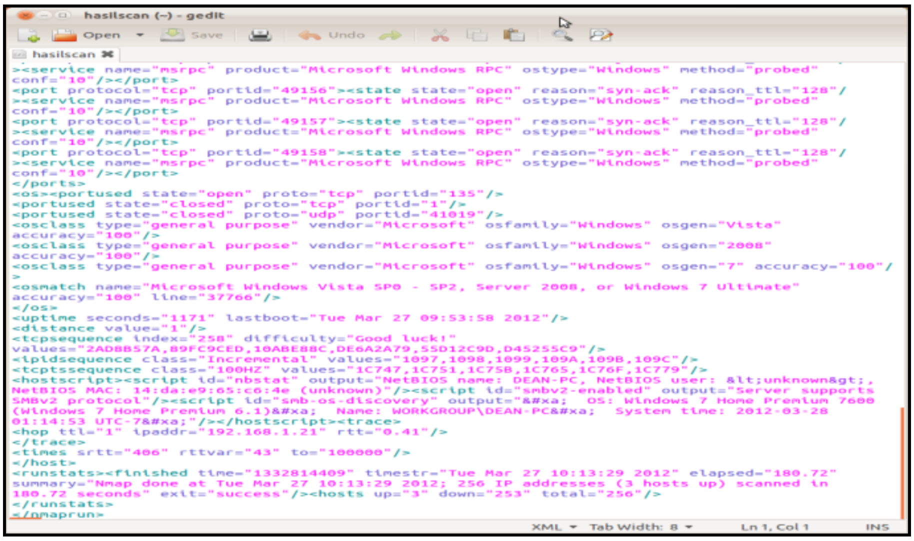
Detail by Signatures

Num	Prio	Signature	# Alerts	# Sources	# Dest.	Detail
1	3	ICMP PING Windows [sid 382] [arachNIDS 169]	155	1	1	Summary
2	3	ICMP PING [sid 384]	155	1	1	Summary
3	3	ICMP Echo Reply [sid 408]	155	1	1	Summary

Page begun: March 8, 2012, 22:54:53
Page finished: March 8, 2012, 22:54:53

Fig. 4: Snort Example.

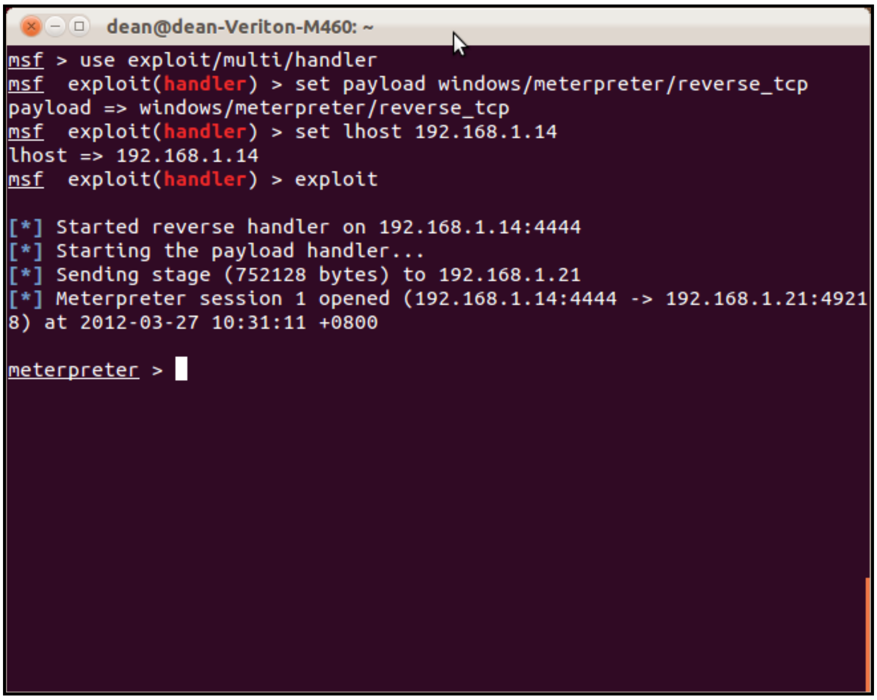
The test on Snort reveals that it successfully record suspicious activities in logs (Fig. 4).



```
><service name="msrpc" product="Microsoft Windows RPC" ostype="Windows" method="probed"
conf="10"/></port>
<port protocol="tcp" portid="49156"><state state="open" reason="syn-ack" reason_ttl="128"/
><service name="msrpc" product="Microsoft Windows RPC" ostype="Windows" method="probed"
conf="10"/></port>
<port protocol="tcp" portid="49157"><state state="open" reason="syn-ack" reason_ttl="128"/
><service name="msrpc" product="Microsoft Windows RPC" ostype="Windows" method="probed"
conf="10"/></port>
<port protocol="tcp" portid="49158"><state state="open" reason="syn-ack" reason_ttl="128"/
><service name="msrpc" product="Microsoft Windows RPC" ostype="Windows" method="probed"
conf="10"/></port>
</ports>
<os><portused state="open" proto="tcp" portid="135"/>
<portused state="closed" proto="tcp" portid="1"/>
<portused state="closed" proto="udp" portid="41019"/>
<osclass type="general purpose" vendor="Microsoft" osfamily="Windows" osgen="Vista"
accuracy="100"/>
<osclass type="general purpose" vendor="Microsoft" osfamily="Windows" osgen="2008"
accuracy="100"/>
<osclass type="general purpose" vendor="Microsoft" osfamily="Windows" osgen="7" accuracy="100"/
>
<osmatch name="Microsoft Windows Vista SP0 - SP2, Server 2008, or Windows 7 Ultimate"
accuracy="100" line="37766"/>
</os>
<uptime seconds="1171" lastboot="Tue Mar 27 09:53:58 2012"/>
<distance value="1"/>
<tcpsequence index="258" difficulty="Good luck!"
values="2ADBB57A,89FC9CED,10ABE88C,DE6A2A79,55D12C9D,D45255C9"/>
<ipidsequence class="Incremental" values="1097,1098,1099,109A,109B,109C"/>
<tcptssequence class="100HZ" values="1C747,1C751,1C75B,1C765,1C76F,1C779"/>
<hostscript><script id="nbstat" output="NetBIOS name: DEAN-PC, NetBIOS user: &lt;unknown&gt;,
NetBIOS MAC: 14:da:e9:65:c6:4e (unknown)"/><script id="smbv2-enabled" output="Server supports
SMBv2 protocol"/><script id="smb-os-discovery" output="&#xa;  OS: Windows 7 Home Premium 7600
(Windows 7 Home Premium 6.1)&#xa;  Name: WORKGROUP\DEAN-PC&#xa;  System time: 2012-03-28
01:14:53 UTC-7&#xa;"/></hostscript><trace>
<hop ttl="1" ipaddr="192.168.1.21" rtt="0.41"/>
</trace>
<times srtt="406" rttvar="43" to="100000"/>
</host>
<runstats><finished time="1332814409" timestr="Tue Mar 27 10:13:29 2012" elapsed="180.72"
summary="Nmap done at Tue Mar 27 10:13:29 2012; 256 IP addresses (3 hosts up) scanned in
180.72 seconds" exit="success"/><hosts up="3" down="253" total="256"/>
</runstats>
</nmaprun>
```

Fig. 5: Nmap XML Output.

Characteristics of an attacking PC are obtained by Nmap.



```
msf > use exploit/multi/handler
msf  exploit(handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf  exploit(handler) > set lhost 192.168.1.14
lhost => 192.168.1.14
msf  exploit(handler) > exploit

[*] Started reverse handler on 192.168.1.14:4444
[*] Starting the payload handler...
[*] Sending stage (752128 bytes) to 192.168.1.21
[*] Meterpreter session 1 opened (192.168.1.14:4444 -> 192.168.1.21:4921
8) at 2012-03-27 10:31:11 +0800

meterpreter >
```

Fig. 6: Reserve TCP Attack by Metasploit.

Test also reveals that Metasploit is successful in disabling and reversing attacks.

Conlusion and Future Work:

This paper has proposed a design for network security tool based on four components namely *Firewall*, *Network Intrusion Detection*, *Vulnerability Scanner* and *Exploit Tool*. The feasibility of this design was demonstrated by the implementation of *Network Defender*, a network security tool, comprised of four open-source applications: *PfSense*, *Snort*, *Nmap* and *Metasploit*. Test results show that all components work well together in detecting and disabling network attacks. The use of Metasploit also enable reverse attacks to be carried out.

Future work include the inclusion of other tools and applications such as SMS alerts and centralized database to better equipped *Network Defender* against attacks. It is hoped that this study has provided a cheaper alternative to SMEs in guarding their network.

REFERENCES

Bhavya Daya, 2013. “Network Security: History, Importance, and Future”. University of Florida Department of Electrical and Computer Engineering. http://web.mit.edu/~bdaya/www/Network%20Security.pdf.

BSD Perimeter LLC, 2004-2011. PfSense. http://www.PfSense.org/.

Firewall (computing), 2013.http://en.wikipedia.org/wiki/Firewall_%28computing%29.

Gordon Fyodor Lyon, 2013. “Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning”. http://Nmap.org/book/.

Host-based Intrusion Detection System, 2013. http://en.wikipedia.org/wiki/Host-based_intrusion_detection_system.

IBM Internet Security Systems (ISS) 2013. 1999-2011. http://www.proventiaworks.com/RealSecure-Server-Sensor.asp.

InterN0T&TheUnkwon, 2007 - Forever. Nmap and Metasploit.http://forum.intern0t.net/general-hacking-discussions/2274-Nmap-Metasploit.html.

Jan Pechanec, 2013. “How the SCP protocol works”. http://en.wikipedia.org/wiki/Secure_copy.

Log Monitoring, 2013.http://en.wikipedia.org/wiki/Log_monitor.

Network Intrusion Detection System, 2013. http://en.wikipedia.org/wiki/Network_intrusion_detection_system.

Network Working Group of the IETF, 2013. “The Secure Shell (SSH) Authentication Protocol”. http://en.wikipedia.org/wiki/Secure_shell.

Radware, 2013.http://www.radware.com/Products/ApplicationNetworkSecurity/.

SecureHost, 2013.http://intrusion.com/products/securehost/.

SNORT, 2013.http://www.Snort.org/.

SourcefireNGIPS/NGFW, 2013. http://www.sourcefire.com/products/next-generation-network-security/ngips-ngfw-features.

StillSecure,2013.http://www.stillsecure.com/press-release/latest-release-stillsecure%C2%99-border-guard-provides-increased-efficiency-and-scalability.